OUCH! 2025. június

SANS SECURITY AWARENESS

Malware elleni védekezés: a láthatatlan ellenség

Egy ártatlan e-mail fájdalmas következményekkel

Sarah egy tehetséges szabadúszó grafikus, akinek a kreativitása és megélhetése a laptopjától függ. Egyik délután, a projekthatáridők végének közeledtével járó sietségben, kapott egy e-mail-t egy leendő ügyféltől. A tárgymezőben ez állt: “Izgalmas projekt lehetőség”. A feladó neve ismerősnek tűnt, arra gondolt, hogy egy korábbi ügyfél ajánlhatta be valakinek. Izgatott volt, hogy felfedezze az új munkát, Sarah megnyitotta az emailt. Ott talált egy udvariasan megfogalmazott üzenetet a potenciális projektről, illetve mellékelve egy “ProjektIsmertető.pdf” nevű csatolmányt. Habozás nélkül rákattintott a dokumentumra, arra számítva, hogy egy új feladat részleteit ismerheti meg.

Ekkor még Sarah nem tudta, hogy ezzel az egyszerű kattintással olyan láncreakciót indít el, amely hamarosan tönkreteheti a szakmai- és magánéletét is. A melléklet egy okosan álcázott malware volt, amelyet arra programoztak, hogy láthatatlanul beépüljön a rendszereibe. Az elkövetkezendő napokban Sarah apró változásokat vett észre: a laptopja teljesítménye lecsökkent, az alkalmazásai pedig váratlanul leálltak. Arra gondolt, hogy ezek csak a szokásos, tipikus hibák, amelyek feltehetőleg a készüleke kora és komoly kihasználtsága miatt alakultak ki.

Akárhogyan is, a helyzet hamar komolyra fordult. Sarah megpróbált belépni az online bankjába, hogy ellenőrizze a folyó- és megtakarítási számláit, belépésnél azonban észre vette, hogy a jelszava már nem működött. Pánikba esve felvette a kapcsolatot a bankjával, ahol arról tájékoztatták, hogy nagyobb mennyiségű pénz felvétele történt meg három különböző külföldi számlára. A megtakarításai, amelyet több év kemény munkával gyűjtött össze, eltűnt. Sarah hamarosan rájött, hogy egy olyan malware támadás áldozatává vált, amely megfertőzte a laptopját, kompromittálta az anyagi biztonságát, és potenciálisan még a szakmai hírnevét is veszélyeztette.

Mi az a malware?

A malware egy olyan számítógépes program, amelyet a kiberbűnözők hoztak létre azzal a céllal hogy belépjenek, kárt okozzanak vagy átvegyék az uralmat számítógépes rendszerek vagy mobileszközök felett az áldozatok hozzájárulása vagy tudomása nélkül. A kifejezés a “*malicious*” (azaz rosszindulatú) és a “*software*” (azaz szoftver) szavakból tevődik össze. Már többször hallhattunk vírusokról, férgekről, trójai vírusokról, zsarolóvírusokról és kémszoftverekről is. Ezek mind a rosszindulatú programok típusai.

A malware-ek azért kifejezetten veszélyesek, mert a számítógépünk vagy készülékünk megfertőzése után a támadók teljesen átvehetik az uralmat felettük anélkül, hogy tudnánk róla. Láthatatlanul rögzítheti az aktivitásunkat, beleértve azt is, hogy kivel beszélgetünk, mit mondunk, illetve a belépési adatainkat és jelszavainkat a legfontosabb fiókjainkhoz.

A rosszindulatú programok titokban megszerezhetik az összes fájlunkat, ideértve fényképeket, videókat, vagy érzékeny dokumentumokat. Közel akármilyen rendszert megfertőzhetnek, ideértve okostelefonokat, okosórákat, de akár okosotthonok készülékeit is, mint például egy termosztát vagy ajtózár. Igen, még az Apple iPhone-ok és Mac számítógépek is megfertőződhetnek, ha nem gondoskodunk megfelelően a biztonságukról.

Védelmünk megerősítése: biztonsági tervek kidolgozása

Szerencsére számos egyszerű lépés van, amit ma megtehetünk, hogy megelőzzük ezeket a támadásokat.

1. **Tartsuk rendszereink naprakészen**: Rendszeresen frissítsük az operációs rendszereinket, alkalmazásainkat és mobil applikációinkat hogy biztosak legyünk abban, hogy az ismert sérülékenységeket javították és a legfrissebb biztonsági funkciókkal rendelkeznek. Ennek legegyszerűbb módja ha engedélyezzük az automatikus frissítéseket.
2. **Legyünk óvatosak az e-mailekkel és üzenetekkel**: Az egyik leggyakoribb mód, amellyel a kiberbűnözők megfertőzik készülékeinket az az, hogy rávesznek minket egy fertőzött melléklet megnyitására, vagy egy fertőzött szoftver letöltésére, esetleg arra, hogy rákattintsunk egy rosszindulatú linkre. Legyünk óvatosak azokkal az üzenetekkel, amelyek sürgetnek minket, vagy olyan üzenetet közvetítenek, amely túl szép ahhoz, hogy igaz legyen.
3. **Használjunk erős, különleges jelszavakat**: A jelszavaink jelentik a birodalmaink kapuit. Ha egy kiberbűnöző kompromittál egyet, átvehetik a hatalmat és megfertőzhetik a készülékünket vagy fiókunkat. Védjük minden eszközünket egy különleges, erős jelszóval vagy jelmondattal. A jelszó hossza kritikus fontosságú. Amikor csak lehetőség van rá, engedélyezzük a többfaktoros hitelesítést (MFA-t vagy 2FA-t).
4. **Csak megbízható forrásokat használjunk letöltésekhez**: Szoftvereket, média anyagokat, illetve applikációkat csak a hivatalos weboldaldalaikról illetve megbízható forrásokból töltsük le. A támadók gyakran úgy fertőzik meg készülékeinket, hogy rávesznek minket arra, hogy olyan nem hivatalos mobilapplikációkat töltsünk le, amelyeket arra fejlesztettek, hogy átvegyék az eszközeink felett a hatalmat.
5. **Használjunk antivírus szoftvereket**: Amikor csak lehetséges, használjunk antivírus megoldásokat, és állítsuk be rajtuk az automatikus frissítést. Nem minden rendszer vagy készülék képes az antivírusok futtatására, továbbá egy antivírus sem képes minden malware megfékezésére, de segíthet.

Vendégszerkesztő

Sherry Peng jelenleg az Agora biztonsági vezetője. A karrierjét helyi önkormányzatoknál kezdte, majd az Információbiztonsági/Kiberbiztonsági mesterdiplomájának megszerzését követően a magánszektorban folytatta azt. Sherry közel 10 éve dolgozik biztonsági területen, és jelenleg a WiCyS Colorado elnöke.

Források

A jelmondatok ereje: https://www.sans.org/newsletters/ouch/power-passphrase/
A jelszókezelők ereje: https://www.sans.org/newsletters/ouch/power-password-managers/
A frissítés ereje: https://www.sans.org/newsletters/ouch/power-updating/
A letöltések veszélye: hogyan járj túl a rosszindulatú mobilapplikációk eszén:
https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps/

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)